ABSTRACT

Secret information is shared by a group of members by giving each member a first share of the information. To reconstruct the secret information, a subgroup consisting of some or all of the members generate second shares from their first shares, and distribute the second shares to the other members of the subgroup. Each member of the subgroup performs an operation on the second shares it receives and one second share it generated itself to obtain an intermediate result. The intermediate results are transmitted to one or more members of the subgroup, or to a central facility, where the original secret information is obtained from a further operation performed on the intermediate results. The original secret information can thereby be obtained without compromising the secrecy of the first shares, and without forcing the members to reveal their identities.